REMARKS/ARGUMENTS

Claims 1-22 are currently pending in this application. Claims 1, 3, 5, 11, 12, and 22 have been amended. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reconsideration, reexamination, and an early indication of allowance of claims 1-22 are respectfully requested.

The Examiner objects to the specification due to certain informalities. The specification has been amended as suggested by the Examiner and thus overcomes the objection. Accordingly, withdrawal of the objection is respectfully requested.

Claims 1, 3, 11, 12, 22, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Applicant submits that the amendments to these claims overcome the rejection under 35 U.S.C. 112, second paragraph, and withdrawal of the rejection is therefore respectfully requested.

Claims 1-3 and 9-10 are rejected under 35 U.S.C. 102(b) as being anticipated by European Patent Publication No. EP 0895164 (Vano). Claims 4-8 and 11-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vano in view of Schneider ("Applied Cryptography," Ch. 17, pp. 397-398). Applicant respectfully traverses these rejections.

Independent claim 1, as amended, recites "an encryption accelerator . . . including a state memory . . . wherein the state memory is initialized with an incrementing pattern without loading the incrementing pattern from an external memory." Independent claim 11, as amended, recites "an encryption

accelerator . . . comprising . . a state memory array . . . and a state machine . . . that directs, storing of an incrementing pattern in the state memory array without loading the incrementing pattern from an external memory." None of the cited references teach or suggest this limitation.

As acknowledged by the Examiner, Vano fails to disclose an encryption accelerator that stores an incrementing pattern in the state memory array. The Examiner, however relies on the disclosure in Schneier to make up for this deficiency. Specifically, the Examiner relies on pages 397-398 of Schneier which disclose the use of an 8*8 S-box: S0, S1, . . ,S255. The S-box is initialized by filling it linearly as follows: S0=0, S1=1, . . . S255=255.

However, nothing in Schneier teaches or suggests that a "state memory is initialized with an incrementing pattern without loading the incrementing pattern from an external memory" as is recited in claim 1. In fact, there is nothing in Schneier or in any of the cited references that teaches or suggests that the initializing of the S-box disclosed by Schneier occurs in a manner that is different from what is conventional in the prior art as described in Applicant's Description of the Prior Art on page 2, lines 17-30. As described there, a conventional encryption/decryption system "includes a CPU 102 coupled to a first memory array 104 used to store a secret key(s) and a second memory array 106 used to store an incrementing pattern by way of an interface 108 . . . In order to encrypt the message 114, . . . the CPU 102 performs a mixing operation by, at 202, storing an incrementing pattern

in the second memory array 106 and a secret key (or keys) in the first memory array 104. Next, at 204, the CPU 102 performs a shifting operation based upon the key values stored in the first memory array 104 and at 206 updates the state array 110 thereby completing the mixing operation . . . The use of a CPU based encryption/decryption system requires a substantial amount of CPU resources thereby severely restricting the CPU for other purposes." Thus, Applicant respectfully submits that claims 1 and 11 are now in condition for allowance.

Claims 2-10 and 12-22 are also in condition for allowance because they depend on an allowable base claim, and for the additional limitations that they contain.

In view of the above amendments and remarks, reconsideration, reexamination, and an early indication of allowance of claims 1-22 are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Josephine E. Chang
Reg. No. 46,083
626/795-9900

JEC/lal
JEC PAS612578.1-*-05/9/05 4:37 PM